



Atty. Dkt. No. 043034-0181

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Masao SHIMADA
Title: NETWORK INFORMATION DETECTION APPARATUS AND METHOD
Appl. No.: 10/802,738
Filing Date: 03/18/2004
Examiner: Unknown
Art Unit: Unknown

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application No. 2003-074846
filed 03/19/2003.

Respectfully submitted,

Date: April 30, 2004

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

By Thomas S. Blumenthal Reg. No. 43,438

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

05

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 1 9 日
Date of Application:

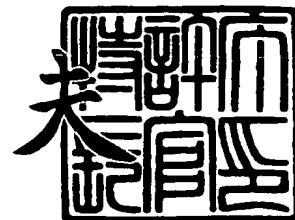
出 願 番 号 特 願 2 0 0 3 - 0 7 4 8 4 6
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 7 4 8 4 6]

出 願 人 日 本 電 気 株 式 有 限 公 司
Applicant(s):

2 0 0 4 年 1 月 1 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 1 1 0 6 0 3

【書類名】 特許願

【整理番号】 34403245

【提出日】 平成15年 3月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/28

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 嶋田 昌生

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100097157

 【弁理士】

 【氏名又は名称】 桂木 雄二

【手数料の表示】

 【予納台帳番号】 024431

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9303562

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク情報検出装置および方法

【特許請求の範囲】

【請求項 1】 ネットワークに接続されたデバイスの IP (Internet Protocol) アドレスを検出するネットワーク情報検出装置において、

前記ネットワーク上の可能な IP アドレスから予め定められた個数ごとに選択された IP アドレスから検査対象 IP アドレスを検出する検査対象検出手段と、

前記検出された検査対象 IP アドレスから目的とする対象デバイスの IP アドレスを検出する IP アドレス検出手段と、

前記ネットワーク上の可能な IP アドレスのすべてについて選択された場合および前記目的とする対象デバイスの IP アドレスが検出された場合のいずれかの場合にネットワーク情報検出動作を終了する制御手段と、

を有することを特徴とするネットワーク情報検出装置。

【請求項 2】 前記 IP アドレス検出手段は、DNS (Domain Name System) サーバの IP アドレスを検出する DNS サーバ検出手段およびルータの IP アドレスを検出するルータ検出手段のうち少なくとも一方を含むことを特徴とする請求項 1 記載のネットワーク情報検出装置。

【請求項 3】 前記 IP アドレス検出手段は、さらに、DNS サーバおよびルータ以外のサービスを提供するデバイスの IP アドレスを検出するサービス検出手段を含むことを特徴とする請求項 2 記載のネットワーク情報検出装置。

【請求項 4】 少なくとも DNS (Domain Name System) サーバを含むネットワーク上の IP (Internet Protocol) アドレスを検出するネットワーク情報検出装置において、

前記ネットワーク上の可能な IP アドレスから 1 以上の検査対象 IP アドレスを検出する検査対象検出手段と、

前記 1 以上の検査対象 IP アドレスに対して DNS クエリメッセージを送信し、そのレスポンスメッセージを受信する DNS メッセージ送受信手段と、

前記レスポンスメッセージから DNS レスポンスメッセージを識別し、DNS レスポンスメッセージから発信元の DNS サーバの IP アドレスを検出する DN

Sサーバ検出手段と、

を有することを特徴とするネットワーク情報検出装置。

【請求項5】 前記検査対象検出手段は、前記ネットワーク内の可能なIPアドレスから予め定められた個数ごとに選択されたIPアドレスに対してARP(Address Resolution Protocol)要求を一括送信し、それに対するARP応答から前記検査対象IPアドレスを検出することを特徴とする請求項4記載のネットワーク情報検出装置。

【請求項6】 前記DNSクエリメッセージは、DNSプロトコルヘッダのQRビットをリセットした、スタンダードクエリ、インバースクエリ、サーバステータスリクエスト、および、アップデートの少なくとも1種類のメッセージであることを特徴とする請求項4記載のネットワーク情報検出装置。

【請求項7】 前記1以上の検査対象IPアドレスに対してICMPエコー要求メッセージを送信し、そのICMPレスポンスメッセージを受信するICMPメッセージ送受信手段と、

前記ICMPレスポンスメッセージから発信元のルータのIPアドレスを検出するルータ検出手段と、

をさらに有することを特徴とする請求項4または5に記載のネットワーク情報検出装置。

【請求項8】 前記ICMPレスポンスメッセージはICMP経路変更要求メッセージおよびICMP時間切れメッセージのいずれかであることを特徴とする請求項7記載のネットワーク情報検出装置。

【請求項9】 ネットワークに接続されたデバイスのIP(Internet Protocol)アドレスを検出するネットワーク情報検出方法において、

前記ネットワーク上の可能なIPアドレスから予め定められた個数ごとに選択し、

前記選択された予め定められた個数のIPアドレスから検査対象IPアドレスを検出し、

前記検出された検査対象IPアドレスから目的とする対象デバイスのIPアドレスを検出し、

前記ネットワーク上の可能な I P アドレスのすべてについて選択された場合および前記目的とする対象デバイスの I P アドレスが検出された場合のいずれかの場合にネットワーク情報検出動作を終了する、

ことを特徴とするネットワーク情報検出方法。

【請求項 1 0】 少なくとも D N S (Domain Name System)サーバを含むネットワーク上の I P (Internet Protocol)アドレスを検出するネットワーク情報検出方法において、

前記ネットワーク上の可能な I P アドレスから 1 以上の検査対象 I P アドレスを検出し、

前記 1 以上の検査対象 I P アドレスに対して送信された D N S クエリメッセージに対するレスポンスメッセージを受信し、

前記レスポンスメッセージから D N S レスポンスメッセージを識別して当該 D N S レスポンスメッセージから発信元の D N S サーバの I P アドレスを検出する、

を有することを特徴とするネットワーク情報検出方法。

【請求項 1 1】 前記検査対象 I P アドレス検出ステップは、

前記ネットワーク内の可能な I P アドレスから予め定められた個数ごとに選択された I P アドレスに対して A R P (Address Resolution Protocol)要求を一括送信し、

前記 A R P 要求に対する A R P 応答から前記検査対象 I P アドレスを検出する、

ことを特徴とする請求項 1 0 記載のネットワーク情報検出方法。

【請求項 1 2】 コンピュータに、ネットワークに接続されたデバイスの I P (Internet Protocol)アドレスを検出するネットワーク情報検出動作を指令するプログラムにおいて、

前記ネットワーク上の可能な I P アドレスから予め定められた個数ごとに選択するステップと、

前記選択された予め定められた個数の I P アドレスから検査対象 I P アドレスを検出するステップと、

前記検出された検査対象 IP アドレスから目的とする対象デバイスの IP アドレスを検出するステップと、

前記ネットワーク上の可能な IP アドレスのすべてについて選択された場合および前記目的とする対象デバイスの IP アドレスが検出された場合のいずれかの場合にネットワーク情報検出動作を終了するステップと、

を有することを特徴とするネットワーク情報検出プログラム。

【請求項 13】 コンピュータに、少なくとも DNS (Domain Name System) サーバを含むネットワーク上の IP (Internet Protocol) アドレスを検出するネットワーク情報検出動作を指令するプログラムにおいて、

前記ネットワーク上の可能な IP アドレスから 1 以上の検査対象 IP アドレスを検出するステップと、

前記 1 以上の検査対象 IP アドレスに対して送信された DNS クエリメッセージに対するレスポンスメッセージを受信するステップと、

前記レスポンスメッセージから DNS レスポンスメッセージを識別して当該 DNS レスポンスメッセージから発信元の DNS サーバの IP アドレスを検出するステップと、

を有することを特徴とするネットワーク情報検出プログラム。

【請求項 14】 前記検査対象 IP アドレス検出ステップは、

前記ネットワーク内の可能な IP アドレスから予め定められた個数ごとに選択された IP アドレスに対して ARP (Address Resolution Protocol) 要求を一括送信するステップと、

前記 ARP 要求に対する ARP 応答から前記検査対象 IP アドレスを検出するステップと、

を有することを特徴とする請求項 13 記載のネットワーク情報検出プログラム。

。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はネットワークシステムに係り、特に、ネットワーク情報を自動取得す

るネットワーク情報検出装置および方法に関する。

【0 0 0 2】

【従来の技術】

コンピュータをネットワークに接続するには、ルータの I P (Internet Protocol) アドレスや D N S (Domain Name System) の I P アドレス等のネットワーク情報をコンピュータに設定する必要がある。このようなネットワーク情報は手動で設定することもできるが、人手による設定にはネットワークの知識を必要とし、ネットワーク情報を調査する手間もかかる。また、誤ってネットワーク情報を設定した場合はネットワーク全体を混乱させることもありうる。

【0 0 0 3】

他方、D H C P (Dynamic Host Configuration Protocol) サーバが存在する場合には、ネットワーク情報を D H C P サーバから取得することができるが、このようなネットワーク情報の自動取得を行うには、ネットワーク情報の提供を目的としたサーバを構築しなければならない。

【0 0 0 4】

特開 2 0 0 2 - 1 9 0 8 1 1 号公報には、ネットワーク上の装置の I P アドレスを自動的に取得する方法の一例が開示されている。この従来の方法では、ネットワーク情報を D H C P サーバから取得できない場合に、ネットワーク・トラフィックを分析して有効なサブネットを決定し（段落番号 0 0 1 8 ～ 0 0 2 1）、そのなかで I C M P (Internet Control Message Protocol) ルータセレクションメッセージを用いてデフォルトルータを、S N M P (Simple Network Management Protocol) の D N S 発見要求を用いて D N S サーバをそれぞれ検出している（段落番号 0 0 2 5 ～ 0 0 2 7）。

【0 0 0 5】

【特許文献 1】

特開 2 0 0 2 - 1 9 0 8 1 1 号公報（段落番号 0 0 2 5 ～ 0 0 2 7、要約、図 3 ～ 5）。

【0 0 0 6】

【発明が解決しようとする課題】

しかしながら、特許文献 1 に開示された IP 構成自動取得方法では、RFC 1256 に記述されているルータの IP アドレス検出方法をそのまま用いているだけであり、ルータ検出の高速化については考慮されていない。また、ICMP ルータセレクションをサポートしていないルータが存在するために、従来の方法ではルータを検出できない場合がある。

【0007】

同様に、上記従来の方法では、DNS サーバ検出の高速化についても考慮されていない。また、SNMP の DNS 発見要求をサポートしていない DNS サーバがあるために、DNS サーバを検出できない場合がある。

【0008】

本発明の目的は、ネットワーク情報を提供するサーバ機能を必要とせずに、ネットワーク情報を自動かつ高速で取得することができるネットワーク情報検出装置及び方法を提供することにある。

【0009】

本発明の他の目的は、ネットワーク情報を確実に取得することができるネットワーク情報検出装置及び方法を提供することにある。

【0010】

【課題を解決するための手段】

本発明の第 1 の側面によるネットワーク情報検出装置は、ネットワークに接続されたデバイスの IP (Internet Protocol) アドレスを検出するネットワーク情報検出装置であって、前記ネットワーク上の可能な IP アドレスから予め定められた個数ごとに選択された IP アドレスから検査対象 IP アドレスを検出する検査対象検出手段と、前記検出された検査対象 IP アドレスから目的とする対象デバイスの IP アドレスを検出する IP アドレス検出手段と、前記ネットワーク上の可能な IP アドレスのすべてについて選択された場合および前記目的とする対象デバイスの IP アドレスが検出された場合のいずれかの場合にネットワーク情報検出動作を終了する制御手段と、を有することを特徴とする。

【0011】

本発明の第 2 の側面によるネットワーク情報検出装置は、少なくとも DNS (D

omain Name System)サーバを含むネットワーク上の I P (Internet Protocol) アドレスを検出するネットワーク情報検出装置であって、前記ネットワーク上の可能な I P アドレスから 1 以上の検査対象 I P アドレスを検出する検査対象検出手段と、前記 1 以上の検査対象 I P アドレスに対して D N S クエリメッセージを送信し、そのレスポンスメッセージを受信する D N S メッセージ送受信手段と、前記レスポンスメッセージから D N S レスポンスメッセージを識別し、D N S レスポンスメッセージから発信元の D N S サーバの I P アドレスを検出する D N S サーバ検出手段と、を有することを特徴とする。

【0 0 1 2】

前記検査対象検出手段は、前記ネットワーク内の可能な I P アドレスから予め定められた個数ごとに選択された I P アドレスに対して A R P (Address Resolution Protocol) 要求を一括送信し、それに対する A R P 応答から前記検査対象 I P アドレスを検出することを特徴とする。

【0 0 1 3】

前記 D N S クエリメッセージは、D N S プロトコルヘッダの Q R ビットをリセットした、スタンダードクエリ、インバースクエリ、サーバステータスリクエスト、および、アップデートの少なくとも 1 種類のメッセージであることを特徴とする。

【0 0 1 4】

さらに、前記ネットワーク情報検出装置は、前記 1 以上の検査対象 I P アドレスに対して I C M P エコー要求メッセージを送信しその I C M P レスポンスメッセージを受信する I C M P メッセージ送受信手段と、前記 I C M P レスポンスメッセージから発信元のルータの I P アドレスを検出するルータ検出手段と、を有することを特徴とする。前記 I C M P レスポンスメッセージは I C M P 経路変更要求メッセージおよび I C M P 時間切れメッセージのいずれかであることを特徴とする。

【0 0 1 5】

【発明の実施の形態】

図 1 は本発明によるネットワーク情報検出装置を含むネットワークの一例を示

す概略的構成図である。この例では、ネットワーク伝送路 1 0 に、ネットワーク情報検出装置 2 0、ホスト A 3 0、ホスト B 4 0、DNS サーバ 5 0 およびルータ 6 0 などの複数のネットワークデバイスが接続されている。本発明によるネットワーク情報検出装置 2 0 は、このサブネットから DNS サーバ 5 0 および／またはルータ 6 0 を検出する。

【0 0 1 6】

図 2 は本発明の第 1 実施形態によるネットワーク情報検出装置を示すブロック構成図である。本実施形態によるネットワーク情報検出装置 2 0 は、ネットワーク伝送路 1 0 に接続するためのネットワークインタフェース部 2 1 を有し、ネットワークインタフェース部 2 1 は ARP 要求送信部 2 3、ARP 応答受信部 2 4、ルータ検出部 2 5、DNS サーバ検出部 2 6、および、ネットワーク情報送信部 2 8 に接続され、後述するように IP パケットまたは ARP パケットの送受信を行う。ARP 応答受信部 2 4 は、後述するように、ルータ検出部 2 5 および DNS サーバ検出部 2 6 に接続され、ルータ検出部 2 5、DNS サーバ検出部 2 6 およびネットワーク情報送信部 2 8 はネットワーク情報設定部 2 7 にそれぞれ接続されている。また、ネットワーク情報検出装置 2 0 の全体的動作は制御部 2 2 により制御される。

【0 0 1 7】

ARP 要求送信部 2 3 は、制御部 2 2 の制御の下で、サブネット内の予め定めた個数の IP アドレスに対して一括して ARP 要求パケットを送信する処理を繰り返す（詳しくは後述する）。なお、IP アドレスの構成は図 7 に、ARP 要求パケットのフォーマットは図 1 1 にそれぞれ示す。

【0 0 1 8】

ARP 応答受信部 2 4 は、ARP 要求送信部 2 3 が送信した ARP 要求パケットに対する ARP 応答パケットをホスト A 3 0、ホスト B 4 0、DNS サーバ 5 0、または、ルータ 6 0 から受信する。当該 ARP 応答パケットの送信元 IP アドレスはルータ検出部 2 5 および DNS サーバ検出部 2 6 へ出力される。ARP 応答パケットのフォーマットは図 1 1 に示す。

【0 0 1 9】

ルータ検出部 2 5 は、A R P 応答受信部 2 4 から入力した送信元 I P アドレスをルータ検出の対象 I P アドレスとし、予め定めた個数のルータ検出対象 I P アドレスごとにルータ特徴確認を繰り返すことによりルータ 6 0 を検出する（詳しくは後述する）。検出されたルータ 6 0 の I P アドレスはネットワーク情報設定部 2 7 に出力される。

【 0 0 2 0 】

D N S サーバ検出部 2 6 は、A R P 応答受信部 2 4 から入力した送信元 I P アドレスを D N S サーバ検出の対象 I P アドレスとし、予め定めた個数の D N S サーバ検出対象 I P アドレスごとに D N S サーバ特徴確認を繰り返すことにより D N S サーバ 5 0 を検出する（詳しくは後述する）。検出された D N S サーバの I P アドレスはネットワーク情報設定部 2 7 に出力される。

【 0 0 2 1 】

ネットワーク情報設定部 2 7 は、ルータ検出部 2 5 が検出したルータ I P アドレスおよび D N S サーバ検出部 2 6 が検出した D N S サーバ I P アドレスの少なくとも一方を、自己の装置に設定したり、または、他のネットワーク装置で利用可能とするためにネットワーク情報送信部 2 8 へ出力する。

【 0 0 2 2 】

ネットワーク情報送信部 2 8 は、ネットワーク情報設定部 2 7 から入力したルータ I P アドレスおよび／または D N S サーバ I P アドレスを他のネットワーク装置で利用可能とするためにネットワークインターフェース部 2 1 を通して送信する。

【 0 0 2 3 】

ネットワーク伝送路 1 0 上を流れるパケットは、たとえば L A N が Ethernet（登録商標、IEEE802.3）であれば図 8 に示すフォーマットのデータリンク層のパケットとなり、I P パケットであれば図 9 に示すフォーマットとなり、A R P パケットであれば図 1 1 に示すフォーマットとなる。

【 0 0 2 4 】

上記ネットワーク情報検出装置 2 0 には、ルータ検出部 2 5 および D N S サーバ検出部 2 6 が両方も受けられているが、一方だけでもよい。

【0025】

なお、図2には図示されていないが、本実施形態によるネットワーク情報検出装置20は、ネットワーク上で上記以外のサービスまたは機能を実行している装置のIPアドレスを検出するサービス検出部を設けることもできる。

【0026】ネットワーク情報検出動作

以下、本実施形態の動作を図3～図5に示すフローチャートおよび図8～図12に示すパケットフォーマットを参照しながら詳細に説明する。

【0027】

図3は本発明による第1実施形態のルータ／DNSサーバ検出動作を全体的に示すフローチャートである。まず制御部22は、予め保存しているサブネット情報に基づいて、ARP要求送信部23がサブネットの全てのIPアドレスに対してARP要求パケット（図11参照）を発行したか否かを判定し（ステップS2001）、真（Yes）の場合は終了する。

【0028】

サブネットの全てのIPアドレスに対してARP要求パケットを発行していない場合には（ステップS2001のNo）、サブネット内の予め定めた個数のIPアドレスごとにARP要求パケットを一括送信する（ステップS2002）。具体的には、サブネットマスクが255. 255. 255. 0、ネットワークアドレスが192. 168. 1. 0とし、一括送信するIPアドレス数を100個と仮定すれば、第一回目のステップS2002の実行時には192. 168. 1. 1～192. 168. 1. 100のIPアドレスに対してARP要求パケットを送信し、第二回目の実行時には192. 168. 1. 101～192. 168. 1. 200のIPアドレスに対して、第三回目の実行時には192. 168. 1. 201～192. 168. 1. 254のIPアドレスに対して、それぞれARP要求を送信する。

【0029】

制御部22は、ARP要求の応答として1つ以上のARP応答パケット（図11参照）を受信したかどうかを判定し（ステップS2003）、なんらARP応

答がない場合は（ステップS2003のNo）、ステップS2001に戻る。

【0030】

1つ以上のARP応答パケットを受信した場合は（ステップS2003のYes）、ルータ検出が終了したかどうかを判定する（ステップS2004）。ルータ検出が終了していなければ（ステップS2004のNo）ルータの特徴確認（ステップS2005）を実行し、終了していれば（ステップS2004のYes）ルータ特徴確認をスキップして、DNSサーバ検出が終了したかどうかを判定する（ステップS2006）。

【0031】

DNSサーバ検出が終了していなければ（ステップS2006のNo）DNSサーバの特徴確認（ステップS2007）を実行して、終了していれば（ステップS2006のYes）、DNSサーバの特徴確認をスキップして、ルータおよびDNSサーバを検出したかどうかを判定する（ステップS2008）。

【0032】

ルータおよびDNSサーバを検出した場合には（ステップS2008のYes）、処理を終了する。ルータおよびDNSサーバを検出していない場合には（ステップS2008のNo）、ステップS2001に戻り、以上の動作をサブネットの全てのIPアドレスに対してARP要求パケットを発行するまで、あるいは、ルータおよびDNSサーバを検出するまで、繰り返す。

【0033】

なお、サービス検出部を有する場合には、サブネット内の予め定めた個数のIPアドレスに対してARP要求パケットを一括発行し、その応答であるARP応答パケットに含まれる送信元IPアドレスに対して、サービス検出あるいは機能検出を行ってもよい。

【0034】

（1）ルータ特徴確認

図4は本発明の第1実施形態におけるルータ検出部のルータ特徴確認動作の一例を示すフローチャートである。まず、ルータの検査対象IPアドレスは、ARP応答受信部24が受信した全てのARP応答パケットにそれぞれ含まれる送信

元 IP アドレスである。これらルータ検査対象 IP アドレスを入力すると（ステップ S 2020）、全てのルータ検査対象 IP アドレスに対してルータ特徴確認を行なったかどうかを判定し（ステップ S 2021）、すべて終了していれば（ステップ S 2021 の Yes）、ルータ特徴確認動作を終了する。

【0035】

検査すべきルータ検査対象 IP アドレスが残っていれば（ステップ S 2021 の No）、TTL (Time To Live) が所望の値に設定された ICMP エコー要求パケット（図 10（A）参照）を予め定めた個数のルータ検査対象 IP アドレスへ一括送信する（ステップ S 2022）。ここでは、TTL = 2、すなわち通過可能ルータ段数が 2 であるとする。

【0036】

例えば、ルータ検査対象 IP アドレスが 192. 168. 1. 10～192. 168. 1. 24、および、192. 168. 1. 40～192. 168. 1. 51 で、10 個の IP アドレスに一括してルータの特徴確認を行なう場合には、ステップ S 2022 の実行は、第一回目に 192. 168. 1. 10～192. 168. 1. 19 に対して一括して ICMP エコー要求を送信し、第二回目に 192. 168. 1. 20～192. 168. 1. 24 と 192. 168. 1. 40～192. 168. 1. 44 とに対して一括して ICMP エコー要求を送信し、第三回目に 192. 168. 1. 45～192. 168. 1. 51 に対して一括して ICMP エコー要求を送信する。

【0037】

ICMP エコー要求パケットを一括送信すると、規定時間内に当該 ICMP エコー要求に対する ICMP 経路変更要求メッセージ（図 10（C）参照）を受信したかどうかを判定する（ステップ S 2023）。

【0038】

ICMP 経路変更要求メッセージを受信しなかった場合は（ステップ S 2023 の No）、規定時間内に当該 ICMP エコー要求に対する ICMP 時間切れメッセージ（図 10（B））を受信したかどうかを判定する（ステップ S 2024）。受信しなかった場合は（ステップ S 2024 の No）、ステップ S 2021

に戻る。 規定時間内に I C M P 時間切れメッセージを受信した場合は（ステップ S 2 0 2 4 の Y e s）、当該時間切れメッセージパケットが含む送信元 I P アドレスをルータの I P アドレスであると判断して（ステップ S 2 0 2 5）、ルータ特徴確認動作を終了する。

【 0 0 3 9 】

I C M P 経路変更要求メッセージを受信した場合は（ステップ S 2 0 2 3 の Y e s）、当該経路変更要求メッセージが含むルータ I P アドレスをルータの I P アドレスであると判断して（ステップ S 2 0 2 6）、ルータ特徴確認動作を終了する。

【 0 0 4 0 】

このように、所定の T T L 設定された I C M P エコー要求パケットを送信し、規定時間内に受信した I C M P 経路変更要求や I C M P 時間切れメッセージによってルータ検出を行うために、ルータの高速検出が可能となる。また、ルータは I C M P 時間切れメッセージ機能を必ずサポートしているために、確実なルータ検出が可能となる。

【 0 0 4 1 】

（ 2 ） D N S サーバ特徴確認

図 5 は本発明の第 1 実施形態における D N S サーバ検出部の D N S サーバ特徴確認動作の一例を示すフローチャートである。まず、D N S サーバの検査対象 I P アドレスは、A R P 応答受信部 2 4 が受信した全ての A R P 応答パケットにそれぞれ含まれる送信元 I P アドレスである。これら D N S サーバ検査対象 I P アドレスを入力すると（ステップ S 2 0 4 0）、全ての D N S サーバの検査対象 I P アドレスに対して D N S サーバ特徴確認を行なったかどうかを判定し（ステップ S 2 0 4 1）、すべて終了していれば（ステップ S 2 0 4 1 の Y e s）、D N S サーバ特徴確認動作を終了する。

【 0 0 4 2 】

検査すべき D N S サーバ検査対象 I P アドレスが残っている場合は（ステップ S 2 0 4 1 の N o）、Q R（質問／回答）ビットをリセットした D N S クエリ（図 1 2 参照）を予め定めた個数の D N S サーバ検査対象 I P アドレスに対して一

一括送信する（ステップ S 2 0 4 2）。この Q R ビットをリセットした D N S クエリは、スタンダードクエリ（O P C O D E = 0）、インバースクエリ（O P C O D E = 1）、サーバステータスリクエスト（O P C O D E = 2）、あるいは、アップデート等のクエリメッセージである。

【 0 0 4 3 】

一括送信に関しては、例えば D N S サーバ検査対象 I P アドレスが 1 9 2 . 1 6 8 . 1 . 1 0 ~ 1 9 2 . 1 6 8 . 1 . 2 4、および、1 9 2 . 1 6 8 . 1 . 4 0 ~ 1 9 2 . 1 6 8 . 1 . 5 1 で、1 0 個の I P アドレスに一括して D N S サーバの特徴確認を行なう場合には、第一回目に 1 9 2 . 1 6 8 . 1 . 1 0 ~ 1 9 2 . 1 6 8 . 1 . 1 9 に対して一括して前記 D N S クエリを送信し、第二回目に 1 9 2 . 1 6 8 . 1 . 2 0 ~ 1 9 2 . 1 6 8 . 1 . 2 4 と、1 9 2 . 1 6 8 . 1 . 4 0 ~ 1 9 2 . 1 6 8 . 1 . 4 4 とに対して一括して前記 D N S クエリを送信し、第三回目に 1 9 2 . 1 6 8 . 1 . 4 5 ~ 1 9 2 . 1 6 8 . 1 . 5 1 に対して一括して前記 D N S クエリを送信する。

【 0 0 4 4 】

D N S クエリを一括送信すると、規定時間内に当該 D N S クエリに対する D N S レスポンスを受信したかどうかを判定する（ステップ S 2 0 4 3）。受信しなかった場合は（ステップ S 2 0 4 3 の N o）、ステップ S 2 0 4 1 に戻る。規定時間内に当該 D N S クエリに対する D N S レスポンスを受信した場合は（ステップ S 2 0 4 3 の Y e s）、D N S サーバの I P アドレスは当該 D N S レスポンスパケットが含む送信元 I P アドレスであると判断し（ステップ S 2 0 4 5）、D N S サーバ確認動作を終了する。

【 0 0 4 5 】

このように、D N S プロトコルのクエリメッセージを送信し、規定時間内に受信したそのレスポンスによって D N S サーバを検出するために、D N S サーバの高速検出が可能となる。また、D N S サーバは、受信したクエリメッセージに対するレスポンス機能を必ずサポートしているために、確実な D N S サーバ検出が可能となる。

【 0 0 4 6 】

図6は本発明の第2実施形態によるネットワーク情報検出装置を示すブロック構成図である。本実施形態によるネットワーク情報検出装置20は、ネットワーク伝送路10に接続するためのネットワークインタフェース201と、上述したIPパケットあるいはARPパケットを送受信するための送受信制御部202とを有し、プログラム制御プロセッサ203が上述したネットワーク情報の検出および設定を制御する。

【0047】

プログラム制御プロセッサ203は、プログラムメモリ204に格納されたルータ検出プログラム、DNSサーバ検出プログラム、および、必要なサービス検出プログラムをそれぞれ読み出して実行することにより、上記図3～図5に示すネットワーク情報検出動作を行うことができる。こうして検出されたネットワーク情報はネットワーク情報メモリ205に格納され、自装置へ設定される。あるいは、ネットワーク上の他の装置の設定のために送信される。プログラム制御プロセッサ203により実行されるネットワーク情報検出動作は、図3～図5によりすでに説明した通りであるから、ここでは省略する。

【0048】

【発明の効果】

以上詳細に説明したように、本発明によれば、ネットワーク上の可能なIPアドレスから予め定められた個数のIPアドレスを順次選択し、選択された予め定められた個数のIPアドレスから検査対象IPアドレスを検出し、前記検出された検査対象IPアドレスから目的とする対象デバイスのIPアドレスを検出することで、IPアドレスの高速検出が可能となる。

【0049】

また、本発明によれば、ICMPエコー要求の応答であるICMP経路変更要求やICMP時間切れメッセージによってルータ検出を行うために、ルータの高速検出が可能となる。また、ルータはICMP時間切れメッセージ機能を必ずサポートしているために、確実なルータ検出が可能となる。

【0050】

さらに、本発明によれば、DNSプロトコルのクエリメッセージに対するレス

ポンスによってDNSサーバを検出するために、DNSサーバの高速検出が可能となる。また、DNSサーバは、受信したクエリメッセージに対するレスポンス機能を必ずサポートしているために、確実なDNSサーバ検出が可能となる。

【0051】

このように、DNSサーバのIPアドレスの検出およびルータのIPアドレスの検出を高速に自動で行うため、ユーザの待ち時間が少なく、また、ユーザの手作業でのDNSサーバ／ルータIPアドレスの入力作業が不要となり、また間違えて入力した場合のネットワークの混乱や負荷の増大を防ぐことができる。とくに、本発明によるネットワーク情報検出装置は、販売店で購入してきたネットワーク装置をユーザのネットワークに接続したり、ネットワーク装置がネットワークを移動する場合に有効である。

【図面の簡単な説明】

【図1】

本発明によるネットワーク情報検出装置を含むネットワークの一例を示す概略的構成図である。

【図2】

本発明の第1実施形態によるネットワーク情報検出装置を示すブロック構成図である。

【図3】

本発明による第1実施形態のルータ／DNSサーバ検出動作を全体的に示すフローチャートである。

【図4】

本発明の第1実施形態におけるルータ検出部のルータ特徴確認動作の一例を示すフローチャートである。

【図5】

本発明の第1実施形態におけるDNSサーバ検出部のDNSサーバ特徴確認動作の一例を示すフローチャートである。

【図6】

本発明の第2実施形態によるネットワーク情報検出装置を示すブロック構成図

である。

【図 7】

I P アドレスのフォーマットを示す図である。

【図 8】

イーサネットパケットのフォーマットを示す図である。

【図 9】

I P パケットのフォーマットを示す図である。

【図 1 0】

(A) は I C M P エコー要求／応答パケットのフォーマットを示す図、(B) は I C M P 時間切れ通知パケットのフォーマットを示す図、(C) は I C M P 経路変更要求パケットのフォーマットを示す図である。

【図 1 1】

A R P パケットのフォーマットを示す図である。

【図 1 2】

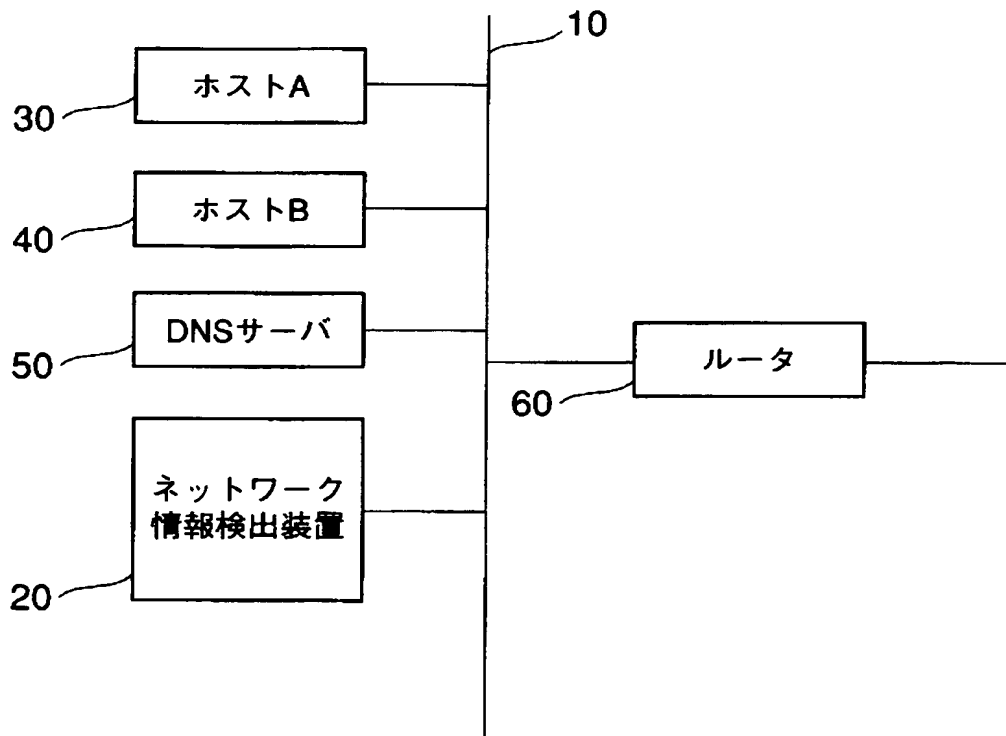
D N S プロトコルヘッダのフォーマットを示す図である。

【符号の説明】

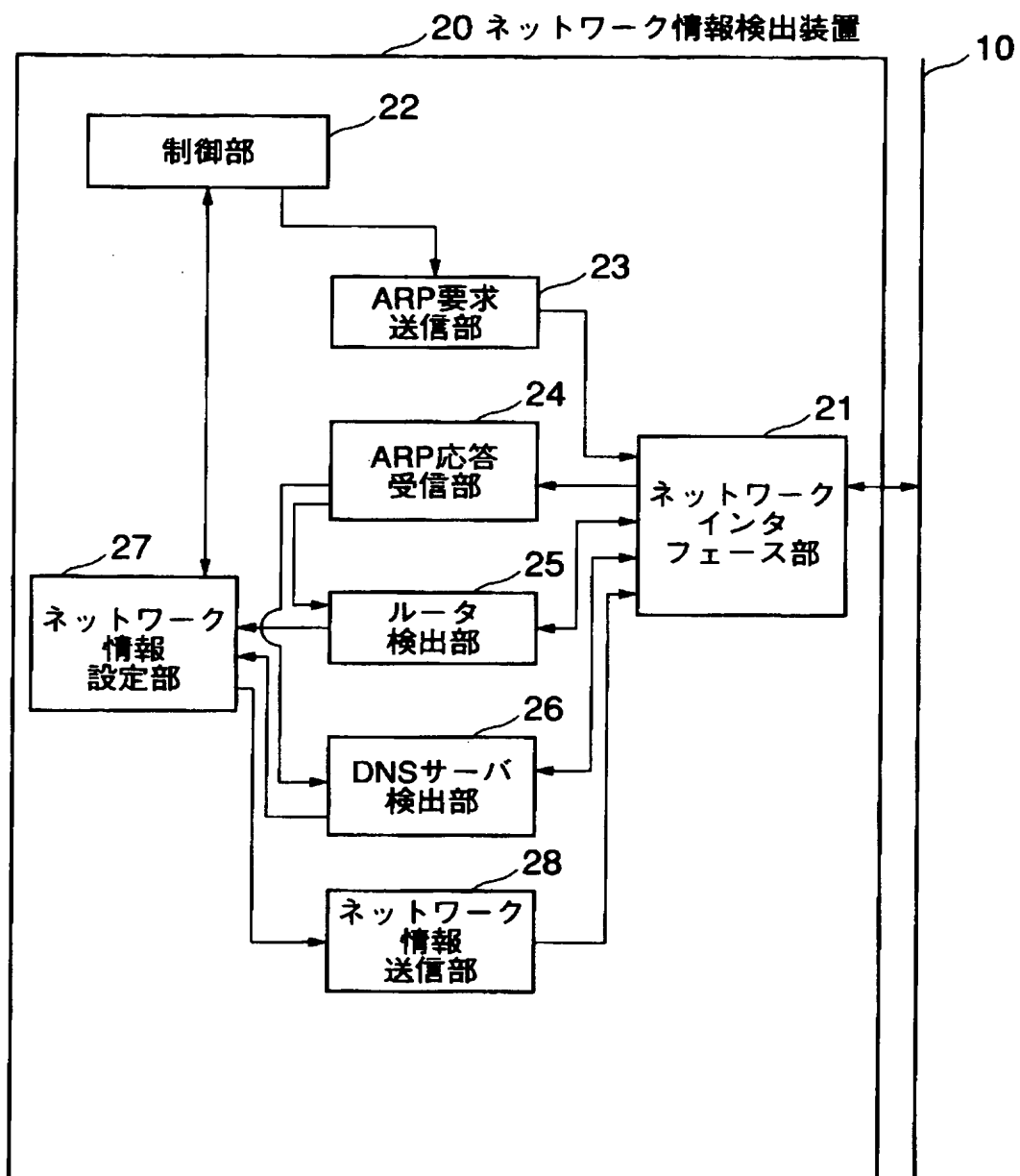
- 1 0 ネットワーク伝送路
- 2 0 ネットワーク情報検出装置
- 3 0 ホスト A
- 4 0 ホスト B
- 5 0 D N S サーバ
- 6 0 ルータ
- 2 1 ネットワークインタフェース部
- 2 3 A R P 要求送信部
- 2 4 A R P 応答受信部
- 2 5 ルータ検出部
- 2 6 D N S サーバ検出部
- 2 7 ネットワーク情報設定部

【書類名】 図面

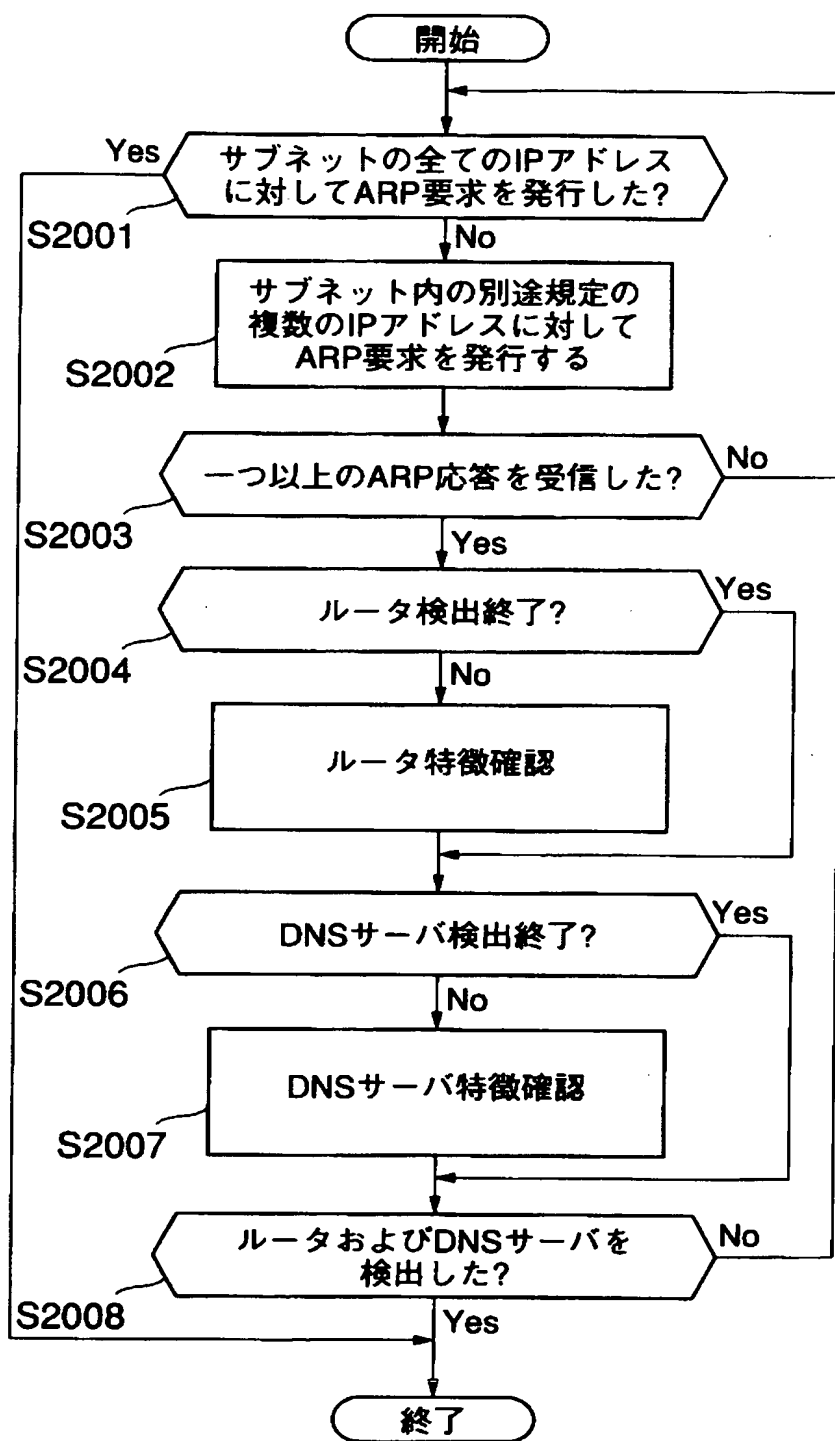
【図 1】



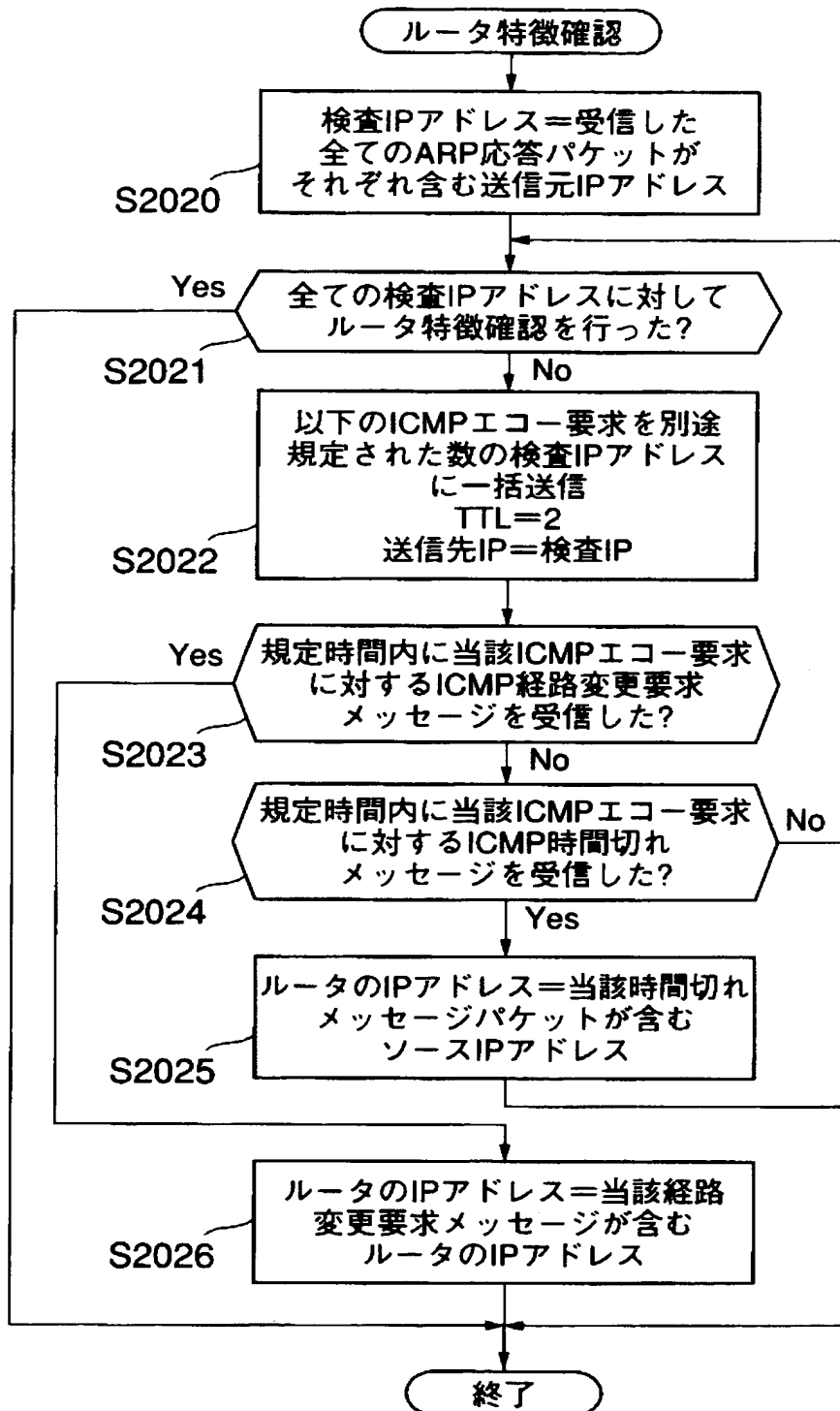
【図 2】



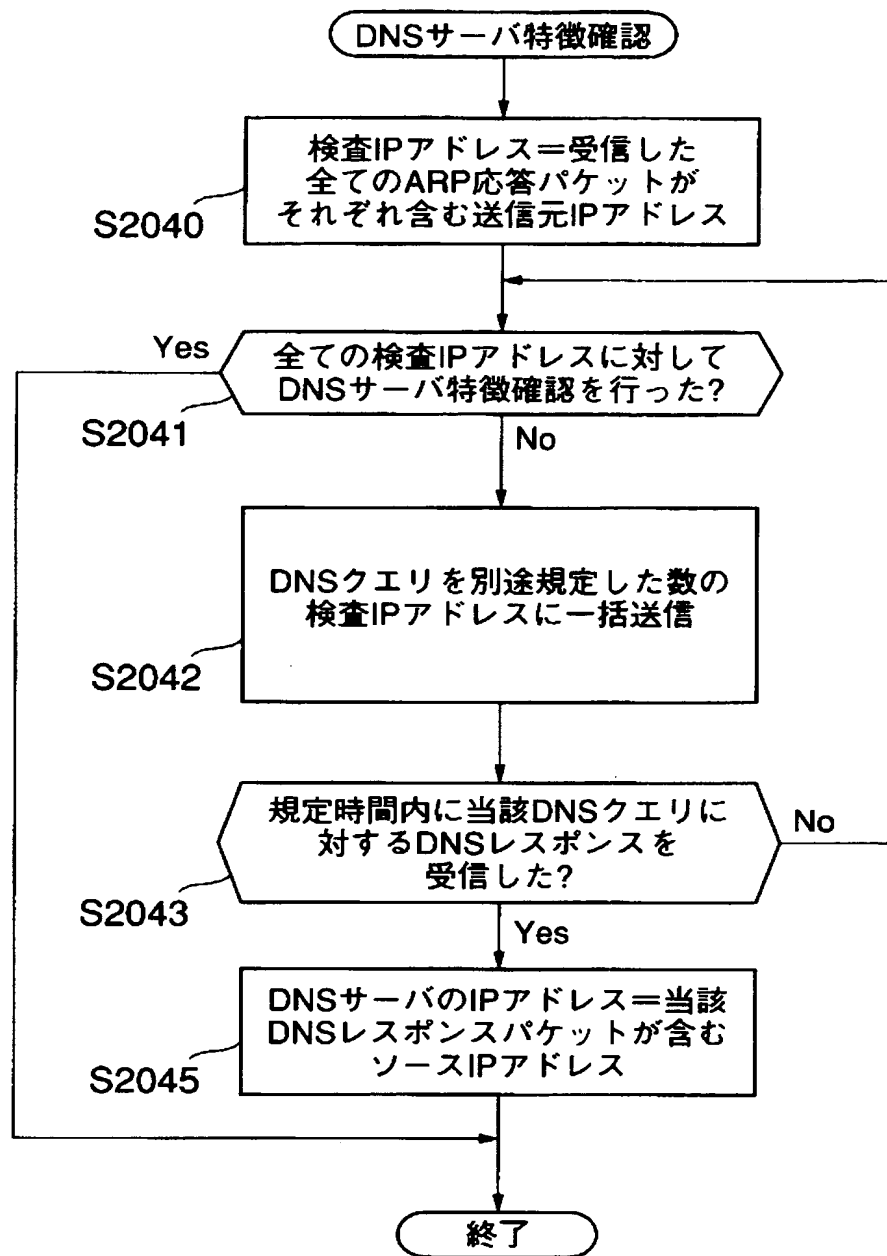
【図 3】



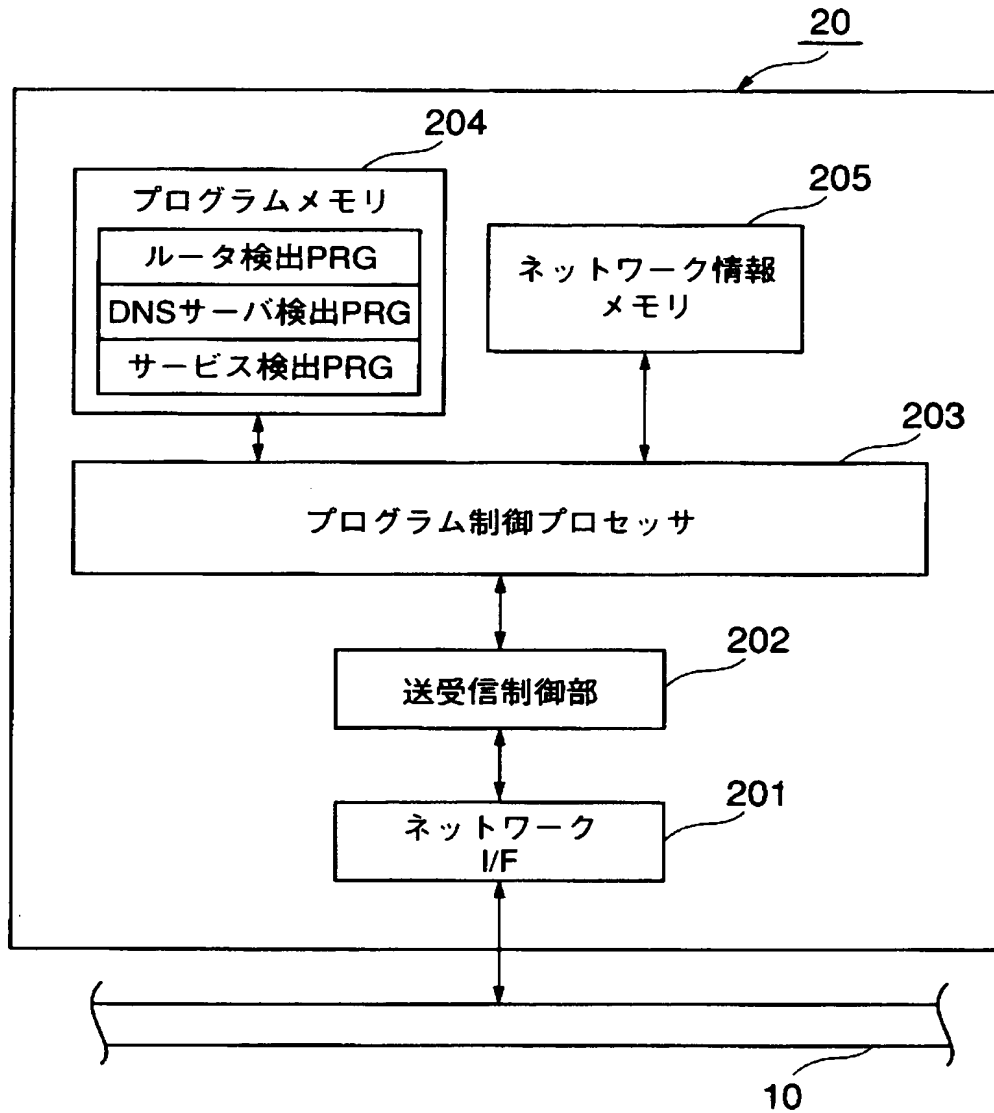
【図 4】



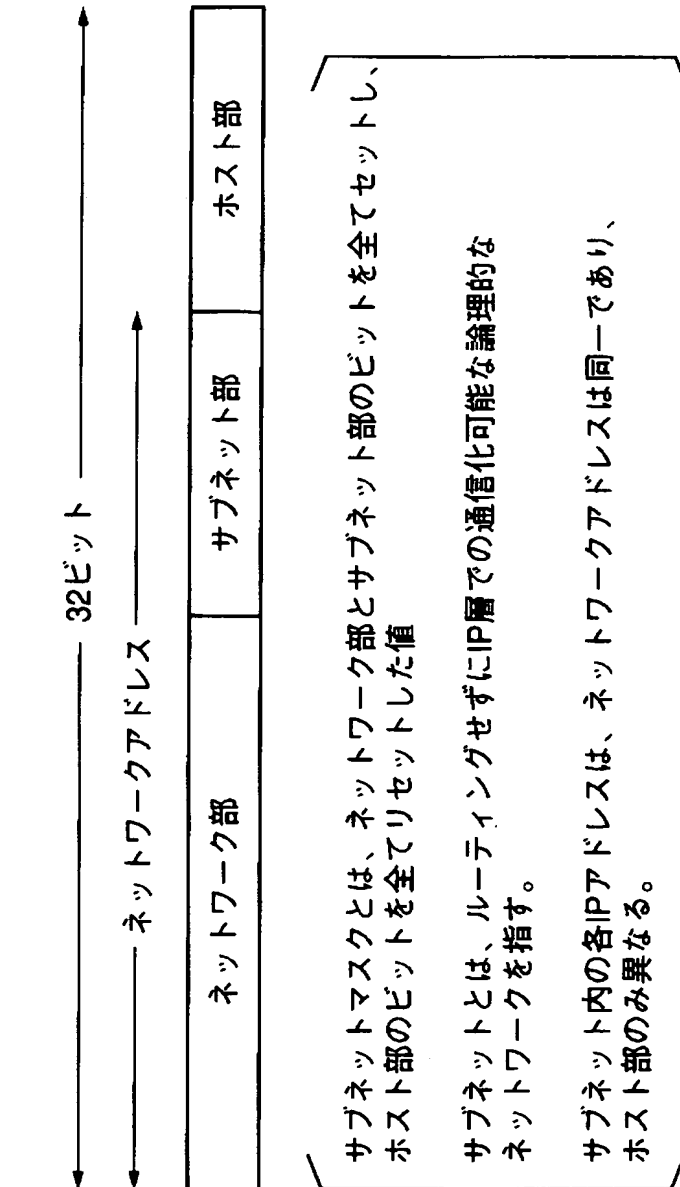
【図 5】



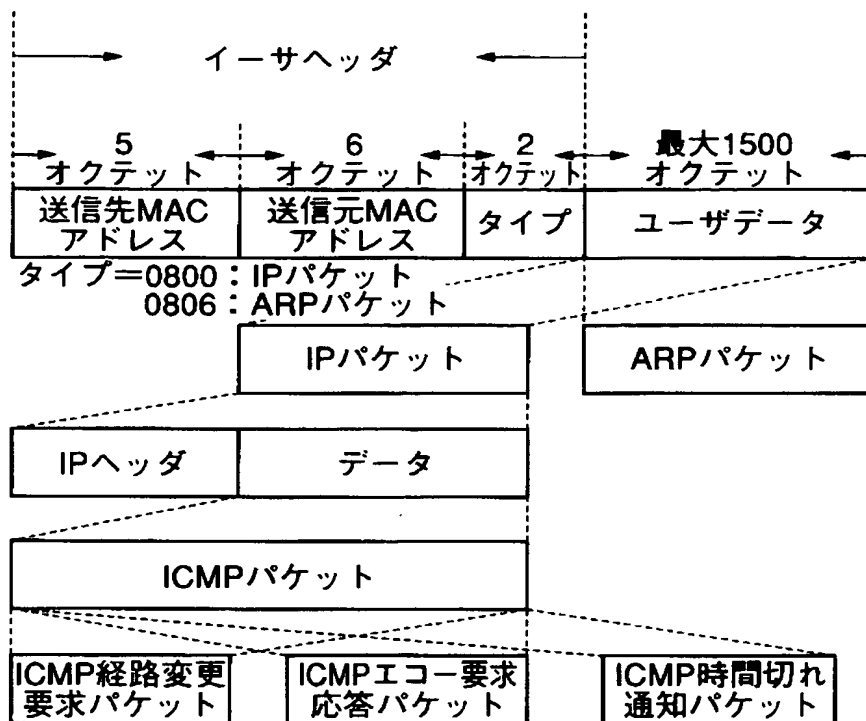
【図 6】



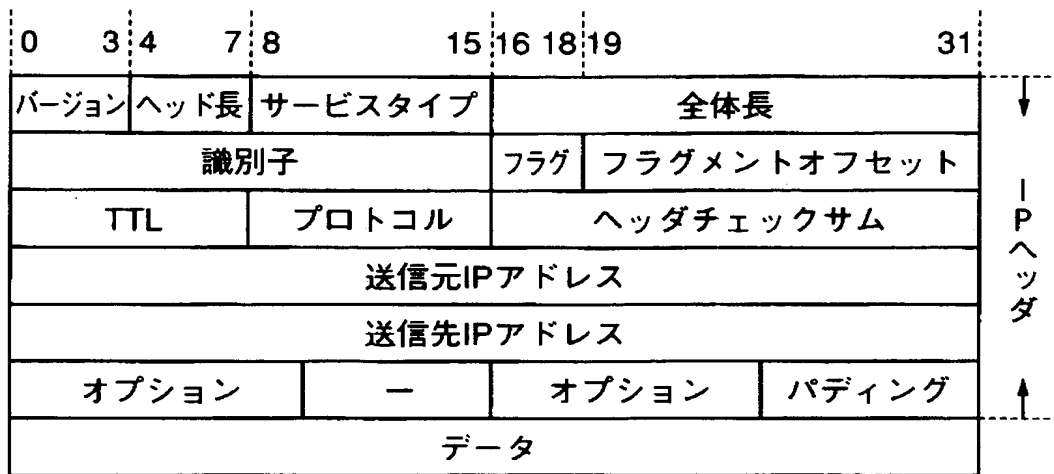
【図 7】



【図 8】

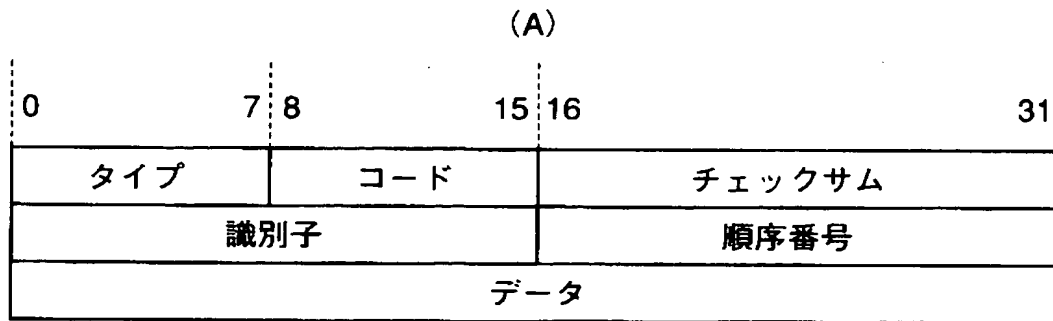


【図 9】

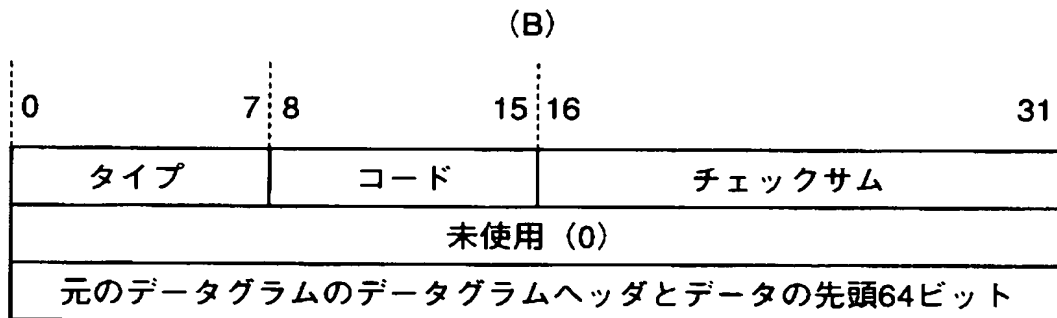


プロトコル=1 : ICMP

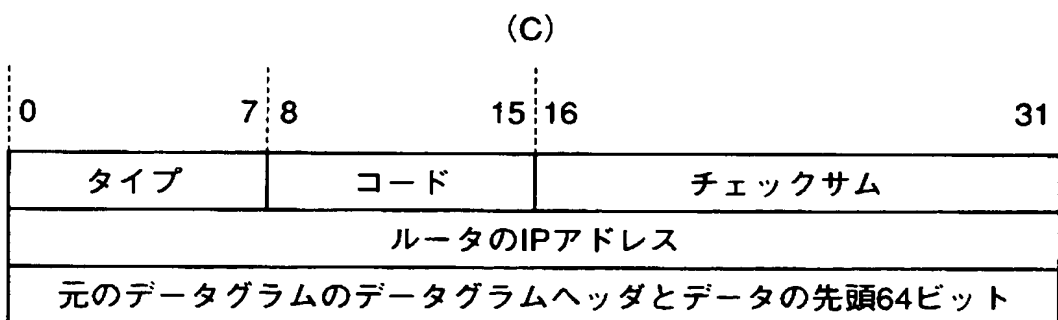
【図10】



タイプ=0: エコー応答 (Echo Reply)
 8: エコー要求 (Echo Request)

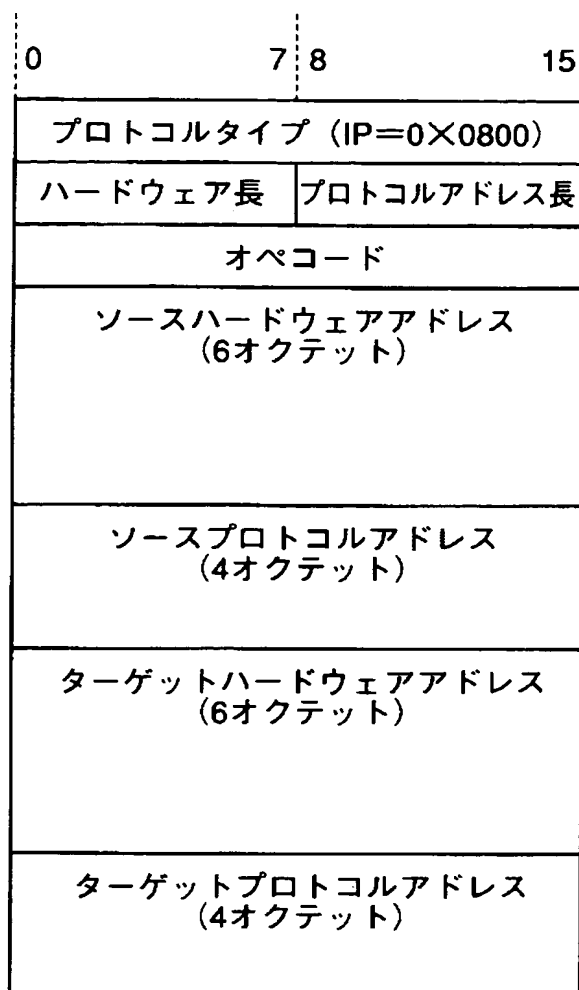


タイプ=11: 時間切れ (Time Exceeded for a Datagram)



タイプ=5: 経路変更要求 (Redirect)

【図 11】



オペコード=1: ARP要求
2: ARP応答
8: InARP要求
9: InARP応答

【図 1 2】

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ID															
QR	Opcode				AA		TC	RD	RA	Z		RCODE			
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

ID : 問い合わせを生成するプログラムによって割当てられた
16ビット識別子。

QR : 質問／回答 このメッセージが質問(0)か回答(1)かを示す
1ビットフィールド。

OPCODE : このメッセージの質問の種類を示す4ビットフィールド。

0

1

2

3・15

a standard query (QUERY)

an inverse query (IQUERY)

a server status request (STATUS)

reserved for future use

【書類名】 要約書

【要約】

【課題】 ネットワーク情報を提供するサーバ機能を必要とせずに、ネットワーク情報を自動かつ高速で取得することができるネットワーク情報検出装置および方法を提供する。

【解決手段】 ネットワーク上の可能な IP アドレスから予め定められた個数ごとに選択された IP アドレスから検査対象 IP アドレスを検出し、検出された検査対象 IP アドレスに対して DNS クエリメッセージおよび ICMP エコー要求メッセージを一括送信する。それらのレスポンスメッセージから DNS サーバおよびルータの IP アドレスを検出する。

【選択図】 図 3

特願 2 0 0 3 - 0 7 4 8 4 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社